

REMARKS

Claims 1-16 are currently pending in the subject application, and are presently under consideration. Claims 1-16 are rejected. Favorable reconsideration of the application is requested in view of the amendments and comments herein.

Claims 1-3, 6-11 and 14-16 have been amended.

I. The Rejection of Claims 1-16 Under 35 U.S.C. §103(a) Should be Withdrawn

Claims 1-16 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Muftic in view of Burn. Withdrawal of this rejection is respectfully requested at least the following reasons.

Claim 1 has been amended to recite creating a certificate and an associated private key, wherein the certificate and the associated private key are wrapped with a public key associated with a token ID and digitally signing the certificate and the associated private key using a signature certificate of a certificate authority (CA) if a match for the token ID and a user signature certificate is found in an authoritative database and decrypting the certificate and the associated private key using a private key stored in the token, such that the token stores at least the token ID, the private key, the user signature certificate and the certificate and the associated private key.

Muftic does not teach or suggest a token storing a user signature certificate, as recited in amended claim 1. The phrase "signature certificate" as recited in amended claim 1, refers to a digital certificate that contains an extension that asserts that the digital signature can be used as a personal digital signature of a user or entity, and that the user or entity providing the signature certificate is the only entity that has a private key matching the public key in the certificate. It is to be appreciated that the signature certificate also contains a signature of a certification authority associated with a public key infrastructure. It is respectfully submitted that the definition of "signature certificate" is well known in the art of public key infrastructures. Muftic discloses

sending a user public key certificate stored on a token with a user identification and a user random number to a network resource (See Muftic Col. 5, Lines 36-38). However, Muftic does not teach or suggest that the user public key certificate could be a signature certificate.

Furthermore, Muftic fails to teach or suggest creating a certificate and an associated private key, wherein the certificate and the associated private key are wrapped with a public key associated with a token ID and digitally signing the certificate and the associated private key using a signature certificate of a CA if a match for the token ID and a user signature certificate is found in an authoritative database, and decrypting the certificate and the associated private key using a private key stored in the token, such that the token stores at least the token ID, the private key, the user signature certificate and the certificate and the associated private key, as recited in amended claim 1. However, in contrast to the contention of the Final Office Action issued on October 4, 2005 (hereinafter "Final Office Action"), the addition of Burn does not cure the deficiencies of Muftic. Since amended claim 1 recites creating a certificate and an associated private key if a match for a token ID and a user signature certificate is found in an authoritative database, it is clear that when the certificate and the associated private key are created, the user signature certificate and the token ID are already in existence. Burn discloses that a CA creates a new key pair for a new user (See Burn, Par. [0044]). Burn also discloses that a new server certification number and a new user certificate are sent to a hardware token processor (HTP) in a registration message encrypted using a non-user-specific certification number generated for the HTP upon initialization (See Burn, Para. [0044]). Burn further discloses that the HTP will decrypt the registration message and store the new certification number and the new user certificate in NV-RAM thereby replacing certificates stored during initialization (See Burn, Para. [0044]). Nothing in Burn teaches nor suggests creating a certificate and an associated private key if a match for a token ID and a user signature certificate is found in an authoritative database, as recited in amended claim 1.

Additionally, as mentioned above, in Burn, when the HTP does store the new certification number and new user certificate, the certificates stored in the HTP during initialization are replaced. Conversely, in amended claim 1, the token recited stores at least two

different certificates, namely a user signature certificate, and a certificate. Thus, Burn also does not teach or suggest decrypting a certificate and an associated private key using a private key stored on a token, such that the token stores at least a token ID, a private key, a user signature certificate and a certificate and an associated private key, as recited in amended claim 1.

Accordingly, taken individually or in combination, Burn and Muftic fail to teach or suggest each and every element of amended claim 1. Thus, Burn and Muftic do not make amended claim 1 obvious, and therefore, amended claim 1 should be patentable.

Claims 2-8 depend either directly or indirectly from amended claim 1 and are patentable over the cited art for substantially the same reasons as amended claim 1, and for the specific elements recited therein. Accordingly, claims 2-8 should be patentable.

Additionally, amended claim 2 recites that a certificate and an associated private key is a plurality of certificates and associated private wherein at least one of the plurality of certificates and associated private keys is a signature certificate for a user, an encryption certificate and associated private key for the user and a role certificate and associated private key for the user, wherein the role certificate includes at least one policy. As admitted in the Final Office Action, neither Muftic nor Burn discloses a role certificate, as recited in amended claim 2 (See Final Action, Page 5). However, in contrast to the contention of the Office Action, Burn also does not suggest a role certificate, wherein the role certificate includes at least one policy as recited in amended claim 2. A policy indicates a limitation on the uses of a role certificate (See Spec. Para. [0024]). Burn discloses that an enrollment request includes a new user's personal identification data including name; address; employee number; social security number; e-mail address and phone and fax numbers, and that the personal information is encrypted and transmitted to a CA (See Burn Para. [0041]). However, Burn does not teach or suggest that any of the personal identification information is stored on an HTP, or that the personal identification information is a policy. That is, Burn does not teach or suggest that a certificate and an associated private is a plurality of certificates and associated private wherein at least one of the plurality of certificates and associated private keys is a signature certificate for a user, an encryption certificate and associated private key for the user and a role certificate and associated private key for the user,

wherein the role certificate includes at least one policy, as recited in claim 2. Accordingly, Muftic and Burn, taken individually or in combination, fail to teach or suggest each and every element of claim 2.

Claim 9 has been amended to recite creating a certificate and an associated private key, wherein the certificate and the associated private key are wrapped with a public key associated with a token ID and digitally signing the certificate and the associated private key using a signature certificate of the certificate authority if a match for the token ID and a user signature certificate is found in an authoritative database and decrypting the certificate and the associated private key using a private key stored in the token, such that the token stores at least the token ID, the private key, the user signature certificate and the certificate and the associated private key. As stated above with respect to amended claim 1, neither Muftic nor Burn, teaches nor suggests creating a certificate and associated private key if a match is found for a token ID and a user signature certificate is found in an authoritative database, as recited in amended claim 9. Accordingly, Muftic and Burn, taken individually or in combination, fail to teach or suggest each and every element of amended claim 9. Thus, Muftic and Burn do not make claim 9 obvious, and therefore, claim 9 should be patentable.

Claims 10-16 depend from amended claim 9 and are patentable over the cited art for substantially the same reasons as amended claim 9 and for the specific elements recited therein. Accordingly, claims 10-16 should be patentable.

Additionally, claim 10 has been amended to recite that a certificate and associated private key is a plurality of certificates and associated private keys wherein at least one certificate and associated private key is a signature certificate for the user, an encryption certificate and associated private key for the user, and a role certificate and associated private key for the user, wherein the role certificate includes at least one policy. As stated above with respect to amended claim 2, neither Muftic nor Burn teaches nor suggests a role certificate that includes at least one policy. Thus, Muftic and Burn taken individually or in combination fail to teach or suggest each and every element of amended claim 10.

Serial No. 10/027,622

Docket No. NG(MS)7194

For the reasons described above, claims 1-16 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

Serial No. 10/027,622

Docket No. NG(MS)7194

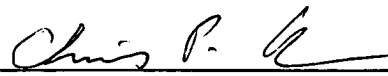
CONCLUSION

In view of the foregoing remarks, Applicant respectfully submits that the present application is in condition for allowance. Applicant respectfully requests reconsideration of this application and that the application be passed to issue.

Please charge any deficiency or credit any overpayment in the fees for this amendment to our Deposit Account No. 20-0090.

Respectfully submitted,

Date 1-25-06



Christopher P. Harris
Registration No. 43,660

CUSTOMER NO.: 26,294

TAROLLI, SUNDHEIM, COVELL, & TUMMINO L.L.P.
526 SUPERIOR AVENUE, SUITE 1111
CLEVELAND, OHIO 44114-1400
Phone: (216) 621-2234
Fax: (216) 621-4072